AMENDMENTS IN THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF THE CLAIMS:

1. (Currently amended) A method of responding to the detection of an intrusion on a network system that provides network services, the network system including one or more attached functions and a plurality of interconnection ~~one or more network infrastructure~~ devices, the method comprising the steps of:

a. establishing signal transfer policies for each of the plurality of interconnection devices;

b. ~~using one or more of the network infrastructure devices to~~ monitoring the network system for intrusions;

c. excluding from at least one of the plurality of interconnection devices a common agent framework for effecting signal transfer policy changes; and

~~b~~d. upon detection of ~~an~~ one or more intrusions of the network, selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices ~~identifying one or more sources of the intrusion;~~

~~c. identifying one or more signal transferring devices of the one or more network infrastructure devices associated with the one or more identified sources; and~~

~~d. configuring the identified one or more signal transferring devices with one or more policy changes~~ in response ~~responsive~~ to the one or more detected intrusions.

2. (Currently amended) The method as claimed in Claim 1 further comprising ~~wherein~~ the step of identifying ~~the~~ one or more sources of the intrusions, including ~~includes~~ the step of identifying a physical address or a logical address of each of the one or more identified sources.

3. (Previously presented) The method as claimed in Claim 2 wherein the physical address information is a MAC address or the logical address information is an IP address.

4. (Currently amended) The method as claimed in Claim 1 further comprising the step of including in at least one of the plurality of interconnection devices the capability for such interconnection devices to change directly their own signal transfer policies ~~wherein the one or more of the network infrastructure devices to monitor the network system is an intrusion detection device~~.

5. (Currently amended) The method as claimed in Claim 4 further comprising the step of employing an intrusion detection device of the network system to perform the function of detecting the one or more intrusions, wherein the intrusion detection device is either a centralized ~~network infrastructure~~ network system device or a plurality of distributed network system devices.

6. CANCELED.

7. CANCELED.

8. (Currently amended) The method as claimed in Claim ~~1~~ 2 further comprising the step of identifying one or more of the plurality of interconnection devices associated with the one or more identified sources of the intrusions, including ~~wherein the step of identifying the one or more signal transferring devices associated with the one or more identified sources includes~~ the step of determining the physical address, logical address, or both for each of the identified one or more interconnection ~~signal transferring~~ devices.

9. (Currently amended) The method as claimed in Claim ~~1~~ 2 further comprising the step of verifying the identification of the identified one or more sources.

10. (Currently amended) The method as claimed in Claim 1 wherein the step of selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions ~~configuring the identified one or more signal transferring devices with one or more policy changes responsive to the detected intrusion~~

includes the step of configuring the ~~identified~~ one or more interconnection ~~signal transferring~~ devices to perform one or more functions selected from the group consisting of: blocking complete access to the network services by ~~the~~ an identified ~~one or more~~ sources of a detected intrusion, blocking access by identified logical addresses only, blocking access by an identified access protocol only, limiting bandwidth, limiting exchanges to or from the ~~identified~~ one or more interconnection ~~signal transferring~~ devices, to or from one or more other devices of the network system ~~infrastructure devices~~, or to or from any of the attached functions not identified as an intrusion source, and directing all signals exchanged by the identified ~~one or more~~ sources to a honeypot, an intrusion detection device, a monitoring device, or a simulation device.

11. (Currently amended) The method as claimed in Claim 1 wherein the step of selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions ~~configuring the identified one or more signal transferring devices with one or more policy changes responsive to the detected intrusion~~ includes the step of configuring the ~~identified~~ one or more interconnection ~~signal transferring~~ devices to permit connectivity of ~~the~~ an identified ~~one or more~~ sources of a detected intrusion while dampening the level of activity associated with the identified ~~one or more~~ sources to minimize network harm while permitting analysis and auditing of the identified ~~one or more~~ sources and the gathering of forensic evidence.

12. (Currently amended) The method as claimed in Claim 1 wherein the step of selectively changing one or more signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions ~~configuring the identified one or more signal transferring devices with one or more policy changes~~ includes the steps of first configuring a first set of the ~~identified~~ one or more interconnection ~~signal transferring~~ devices with a first set of one or more policy changes, monitoring the network system for intrusions and, upon detection of one or more intrusions related to the intrusions causing the first one or more policy changes, configuring a second set of the ~~identified~~ one or more interconnection ~~signal transferring~~ devices with a second set of one or more policy changes.

13. (Currently amended) The method as claimed in Claim 12 wherein one or more of the one or more ~~signal transferring~~ interconnection devices of the second set are ~~signal transferring~~ interconnection devices of the first set.

14. (Currently amended) The method as claimed in Claim 1 wherein the ~~identified~~ one or more interconnection ~~signal transferring~~ devices are ~~selected from the group consisting of~~ network entry devices ~~and centralized switching devices~~.

15. (Currently amended) The method as claimed in Claim 1 wherein the one or more policy changes are configured on one or more ports of one or more of the identified one or more ~~enforcement~~ signal transferring devices.

Claims 16-27: CANCELED.

28. (New) The method as claimed in Claim 1 further comprising the steps of:

a. identifying one or more sources of the intrusions, including the step of identifying a physical address or a logical address of each of the one or more identified sources;

b. identifying one or more network entry devices of the plurality of interconnection devices locally connecting the one or more identified sources of the intrusions to the network system, including the step of determining the physical address, logical address, or both for each of the identified one or more network entry devices.

29. (New) The method as claimed in Claim 28 further comprising the step of verifying the identification of the identified one or more sources.

30. (New) A network system including a plurality of attached functions, and the network system including the capability to respond to intrusions thereof, the network system comprising:

a. an intrusion detection function for identifying one or more sources of one or more intrusions of the network system;

b. a plurality of interconnection devices for transferring signals through the network system, wherein each of the plurality of interconnection devices includes one or more signal transfer policies, and

c. a function to change selectively the signal transfer policies of one or more of the plurality of interconnection devices in response to the one or more detected intrusions,

wherein there is no common agent framework distributed among the plurality of interconnection devices to establish therein either or both of the intrusion detection function and the function to change selectively the signal transfer policies.

31. (New) The network system as claimed in Claim 30, wherein at least one of the interconnection devices has no intrusion detection function and wherein the signal transfer policies of that at least one of the plurality of interconnection devices cannot be changed in response to the one or more detected intrusions.

32. (New) The network system as claimed in Claim 30, wherein at least one of the plurality of interconnection devices includes the function to change directly its own signal transfer policies.

33. (New) The network system as claimed in Claim 30 further comprising a directory service function for receiving address information for the attached functions and the interconnection devices.

34. (New) The network system as claimed in Claim 33 further comprising a policy manager function for configuring the plurality of interconnection devices with the signal transfer policies.

35. (New) The network system as claimed in Claim 34 further comprising a policy decision function configured:

a. to receive detected intrusion information from the intrusion detection function;

b. to receive information from the directory service function;

c. to evaluate whether a policy change or changes is or are required on one or more of the interconnection devices in response to the detected intrusion information; and

d. to direct the policy manager function to configure one or more of the plurality of interconnection devices with determined policy changes upon deciding to do so based upon the evaluation.

36. (New) The network system as claimed in Claim 35 wherein the policy manager function and the policy decision function are part of a centralized server.

37. (New) The network system as claimed in Claim 36 wherein the directory service function is part of the central server.

38. (New) The network system as claimed in Claim 30 wherein the intrusion detection function is a centralized intrusion detection function or a distributed intrusion detection function.

39. (New) The network system as claimed in Claim 30 wherein the one or more of the plurality of interconnection devices selected for signal transfer policies changes are network entry devices selected based on their local connection to the one or more sources of the one or more intrusions.

40. (New) The network system as claimed in Claim 30 further comprising a network management system for identifying address information for the plurality of interconnection devices.

41. (New) The network system as claimed in Claim 30 further comprising a function to validate the accuracy of the identity of the identified one or more sources including a logical address, a physical address, or a location.